International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 10 Oct 2021, pp: 1043-1046 www.ijaem.net ISSN: 2395-5252

Designing and Implementation of Quantum Algorithms

Vikash Babu
Master of Technology Sanskriti University Mathura (UP)

Submitted: 15-10-2021 Revised: 26-10-2021 Accepted: 28-10-2021

ABSTRACT– In this paper , I summarized the basic to intermediate information one need to generate deep understanding about designing and implementation of basic quantum algorithms in mathematical format by some standard derivations and quantum rules from other research papers of quantum mechanics. Topics in this paper covered are like hadamard transformation, hamming distance and weight, Tiffoli gate, ways to measure complexity of quantum algorithm with respect to classical computers. Further in this paper I solved initial problems of quantum and classical domain with this approach like black box or oracle problem.

I. INTRODUCTION

Initially quantum computers and classical computer's algorithms start same way, then we create Quantum parallelism setup. So , we can take advantage of quantum system over classical system. We first establish or create quantum superposition then input it to quantum version of classical gates to calculate function F.This setup is known as Quantum Parallelism Setup.

Till this point quantum algorithm has no merits over classical computing algorithms. Now an algorithm designer have to use quantum parallelism to make a quantum algorithm far superior then classical algorithms.

Hadamard Transformation –

$$H = \frac{1}{\sqrt{2}}(|0\rangle\langle 0| + |1\rangle\langle 0| + |0\rangle\langle 1| - |1\rangle\langle 1|$$

$$H : |0\rangle \rightarrow |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$H : |1\rangle \rightarrow |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

It produce even superposition for both $|0\rangle$ and $|1\rangle$
H.H = 1

For standard basis $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

When we apply Hadamard transformation H to create a superposition of all input values. When we apply in qubits individually with state |0> then H generates a superposition 2^n standard basis vectors. From 0 to 2^n-1

$$(H \otimes H \otimes ---H)|00 --- 0\rangle$$

$$= \frac{1}{\sqrt{2}}(((|0\rangle + |1\rangle)) \otimes (|0\rangle + |1\rangle) \otimes ---(|0\rangle + |1\rangle))$$

$$= \frac{1}{\sqrt{2^n}}(|0 \ldots 00\rangle + |0 \ldots 01\rangle + |1 \ldots 00\rangle + \cdots + |1..11\rangle)$$

$$= \frac{1}{\sqrt{2}}\sum_{x=0}^{2^n} |x\rangle$$

Hamming Distance – Numbers of bit different between two bit string x and y is hamming distance $d_H(x, y)$

No. of 1 bits in x is known as Hamming weight $d_H(x)$

$$d_H(x) = d_H(x, y)$$

⇨ $W = H \otimes H \otimes \ldots \ldots \ldots H$ Which applies H to each Qubit in n- qubit is called Walsh – Hadamard Transformation.

$$W|0\rangle = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1} |x\rangle$$

$$W_{sr} = W_{rs} = \frac{1}{\sqrt{2}}(-1)^{rs}$$

For Quantum parallelism

$$U_f : \sum_x a_x |x, 0\rangle \rightarrow \sum_x a_x |x, f(x)\rangle$$

$$U_f : (W|0\rangle) \otimes |0\rangle$$

$$= \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1} |x\rangle|0\rangle$$

$$\rightarrow \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1} |x\rangle|f(x)\rangle$$

Just by using U_f only once , superposition now ontain all 2^n functional values entangled with their corresponding input value x.

Controlled Controlled Not (Tiffoli) Gate 'T'– This is a single qubit register taking all possible qubit combinations of x and y. register is initially set to 0.

For x & y = 0

$$W(|00\rangle) \otimes |0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle$$

$$W(|00\rangle) \otimes |0\rangle = \frac{1}{2}(|000\rangle + |010\rangle + |100\rangle + |110\rangle)$$

Applying the Tiffoli gate T to this superposition of input fields

$$T(W(|00\rangle) \otimes |0\rangle) = \frac{1}{2}(|000\rangle + |010\rangle + |100\rangle + |111\rangle)$$

Complexity – There are many ways to compute complexity of a quantum circuit or quantum algorithm but we mainly use quantum circuit complexity and quantum query complexity.

- Complexity of a quantum circuit is defined by number of simple gate in circuit.
- Any quantum circuit family C is consistent if its circuit give consistent result.
- Uniformity condition means the circuit construction cant be arbitrarily complex.
- Number of calls required to a function to solve any particular problem is query complexity.
- Number of qubits transferred in order to communicate n bits of information is known as communication complexity.

Some Somple Quantum Algorithms –
Black box / oracle problem by daviddeutech.

David shows that his approach has better query complexity than any possible classical algorithm.

Problem Statement – Given a Boolean function : $z_2 \rightarrow z_2$. determine whether f is constant or not.
We know U_f for a single bit function f , takes two qubits of input and produce two qubits of output/
Input $|x\rangle|y\rangle, U_f \rightarrow |x\rangle|f(x) \oplus y\rangle$
When $|y\rangle = |0\rangle$ then

$$U_f \rightarrow |x\rangle|f(x)\rangle$$

In algorithm we apply Uf to two qubit state $||+\rangle|-\rangle$, where the first qubit is a superposition of two values and third qubit is in superposition $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

$$U_f(|+\rangle|-\rangle) = U_f(\frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle))$$

$$U_f(|+\rangle|-\rangle) = \frac{1}{2}(|0\rangle(|0 \oplus f(0)\rangle + |1 \oplus f(0)\rangle) + |1\rangle(|0 \oplus f(1)\rangle + (1 \oplus f(1)\rangle))$$

$$U_f(|+\rangle|-\rangle) = \frac{1}{2}\sum_{x=0}^{1} |x\rangle(|0 \oplus f(x)\rangle - (1 \oplus f(x)\rangle)$$

$$U_f\left(\frac{1}{\sqrt{2}}\sum_{x=0}^{1} |x\rangle|-\rangle\right) = \frac{1}{\sqrt{2}}\sum_{x=0}^{1}(-1)^{f(x)}|x\rangle|-\rangle$$

Now for f constant $(-1)^{f(x)}$ is physically meaningless global phase , so state is simple $|+\rangle|-\rangle$.
For f not constant $(-1)^{f(x)}$ negates exactly one of the term in superposition so state is $|-\rangle|-\rangle$.
for algorithm, if we apply Hadamard transformation H to first qubit then measure it. We obtain $|0\rangle$ in first case and $|1\rangle$ in second case.
Thus with a single call to Uf we can detramine whether f is constant or not. While in classical computing it will take atleast two calls to solve simplest problem of this domain.

Sub Routine - we haveto untangle temporary or unnecessary qubits in order to avoid errors in computation.
For eg.$V_f : |x, t, y\rangle \rightarrow |x, t \oplus x, y \oplus f(x)\rangle$.
There deutsch's algorithm no longer work.
Begin with $|t\rangle$ in $|0\rangle$ as before first qubit in $|+\rangle$ and third qubit in state $|-\rangle$

$$V_f(|+\rangle|0\rangle|-\rangle) = V_f\left(\frac{1}{\sqrt{2}}\sum_{x=0}^{1}|x\rangle|0\rangle|-\rangle\right) = \frac{1}{\sqrt{2}}\sum_{x=0}^{1}(-1)^{f(x)}|x\rangle|x\rangle|-\rangle$$

First qubit is entangled with second , because of this entanglement applying H to first qubit and then measuring it will not produce desired result like when f is constant
Sate is $(|00\rangle + |11\rangle)|-\rangle$ applying $H \otimes I \otimes I \rightarrow \frac{1}{2}(|00\rangle + |10\rangle - |11\rangle)|-\rangle$ a similar calculation shows when f is inconsistent so we can no longer differentiate both cases. Entanglement of qubit$|t\rangle$ has destroyed quantum computation, to avoid such problems we entangle qubits at the starting of calculation and then by end of subroutine after measuring result we untangle every temporary on further unnecessary qubit, so that at the end of algo they are always in state $|0\rangle$.
For that we have to find a efficient implementation of quantum transformation

$$S_x^{\emptyset}: \sum_{x=0}^{N-1} a_x|x\rangle \rightarrow \sum_{x \in X} a_x\, e^{i\emptyset}|x\rangle + \sum_{x ! \in X} a_x|x\rangle$$

For using any qubit temporarily define phase $f(\emptyset)|x[k]\rangle =$
Qubita[1]

$$U_f|x, a\rangle$$

$$K(^{\emptyset}/_{2})|a\rangle$$
$$T(^{-\emptyset}/_{2})|a\rangle$$
$$U_f^{-1}|x,a\rangle$$

Since

$$T\left(^{-\emptyset}/_{2}\right)K\left(^{\emptyset}/_{2}\right) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\emptyset} \end{pmatrix}$$

Step 3 and 4 shift the phase by $e^{i\emptyset}$ if and only if bit a is one strictly speeking step 3 is a physically meaning less global phase shift. Performing step 3 merely make it easier to get desired result .we can easily replace step 3 and 4 by single step $\cap$ $K(\emptyset)|a\rangle|x_i\rangle$ i can be any qubit in register x.

Special case $\emptyset = \pi S_x^{\pi}$ can be implemented by initializing a temporary qubit b to $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Then using $U_f$compute into this register

$$|\varphi\rangle = \sum_{x\epsilon X} a_x|x\rangle + \sum_{x!\epsilon X} a_x|x\rangle$$

and compute

$$U_f(|\varphi\rangle \otimes |-\rangle) = U_f(\sum_{x\in X} a_x|x\rangle \otimes |-\rangle)$$
$$+ U_f(\sum_{x!\in X} a_x|x\rangle \otimes |-\rangle$$
$$= -(\sum_{x\in X} a_x|x\rangle \otimes |-\rangle) + (\sum_{x!\in X} a_x|x\rangle \otimes |-\rangle$$
$$= (S_X^{\pi}|\varphi\rangle) \otimes |-\rangle$$

Problems

1. Deutsch Jozsa Problem – David deutsch and Richard jozsa presenter a algorithm for multiple bit generalization

Statement – a function f is balanced if an equal number of input values to the function return 0 & 1. $f: Z_{2^n} \rightarrow Z_2$that is known to be either constant or balanced and a quantum oracle.

$U_f : |x\rangle|y\rangle \rightarrow |x\rangle|y \oplus f(x)\rangle$for f , determine whether function is constant or balanced.

Solution – Algorithm first use phase sub routine to compute superposition term of corresponding to bases vectors $|x\rangle$ with $f(x) = 1$

Subroutine return $|\varphi\rangle = \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}(-1)^{f(i)}|i\rangle$.

Now apply Walsh Transformation W to result $|\varphi\rangle$

$$|\varphi\rangle = \frac{1}{N}\sum_{i=0}^{N-1}((-1)^{f(i)}\sum_{j=0}^{N-1}(-1)^{i.j}|j\rangle)$$

For constant f $(-1)^{f(i)} = (-1)^{f(0)}$is simply a global phase and $|\emptyset\rangle$is simply $|0\rangle$

$$(-1)^{f(0)}\frac{1}{2^n}\sum_{i\in z_2^n}(\sum_{j\in Z_2^n}(-1)^{i.j})|j\rangle$$
$$= (-1)^{f(0)}\frac{1}{2^n}\sum_{i\in Z_2^n}(-1)^{i.0}|0\rangle$$
$$= (-1)^{f(0)}|0\rangle$$

And for balanced $\sum_{i\in Z_2^n}(-1)^{i.j} = 0 \quad \& j \neq 0$

$$|\emptyset\rangle = \frac{1}{2^n}\sum_{j\in Z_2^n}(\sum_{i\in X0}(-1)^{i.j} - \sum_{i!\in X0}(-1)^{i.j})|j\rangle$$

Where $X_0 = \{x|f(x) = \}$

This quantum algorithm solves Deutsch Jozsa problem with just one evolution of Uf .while any clasiccal algorithm must evolute f al least $2^{n-1} + 1$times to solve problem with certainity.

2. **Bernstein Vazirani Problem –** Determine the value a unknown bit string ‘u’ of length ‘n’ where algorithm can query in form q*u for query string ‘q’.

Classical algorithm uses O(n) calls to $f(q) = q.u \bmod 2$.

Where as quantum algorithm uses just one call

$$f_u(q) = q.u \bmod 2$$
$$U_{fu} : |q\rangle|b\rangle \rightarrow |q\rangle|b \oplus f_u(q)\rangle$$
$$|\varphi\rangle = \frac{1}{\sqrt{2^n}}\sum_q(-1)^{x.z}|q\rangle = \frac{1}{\sqrt{2^n}}\sum_q(-1)^{u.q}|q\rangle$$

$$W|x\rangle = \frac{1}{\sqrt{2^n}}\sum_z(-1)^{x.z}|Z\rangle$$

Thus

$$W|\varphi X\rangle = W(\frac{1}{\sqrt{2^n}}\sum_q(-1)^{u.q}|q\rangle)$$
$$= \frac{1}{2^n}\sum_q(-1)^{u.q}(\sum_z(-1)^{q.z}|z\rangle$$

We know $(-1)^{u.q+z.q} = (-1)^{(u\oplus z).q}$ and internal sum is 0 unless $u \oplus z = 0$ which means u=z.

$$W(|\varphi x\rangle) = \frac{1}{2^n}\sum_z(\sum_q(-1)^{u.q+z.q})|z\rangle$$

- ➢ In quantimparrallalism we computer all possible input query at the same time with superposition.

3. **Simon’s Problem -** Given a 2 to 1 function f such that $f(x) = f(x \oplus a)$ for all $x \in Z_2^n$. find hidden string $a \in Z_2^n$.

Best classical algorithm can do this task in $O(2^{n}/_{2})$ calls while quantum algorithm takes only one call and $O(n^2)$ steps.

First create a superposition a $\sum_x|x\rangle\,|f(x)\rangle$.

Now apply Walsh Hadamard Transformation W

$$W(\frac{1}{\sqrt{2}}(\ |x_0\rangle + |x_0 \oplus a\rangle))$$

$$= \frac{1}{\sqrt{2}}(\frac{1}{\sqrt{2^n}}\sum_{y}(-1)^{x0.y} + (-1)^{(x0\oplus a).y})|y\rangle)$$

$$= \frac{1}{\sqrt{2^{n+1}}}\sum_{y}(-1)^{x0.y}(1 + (-1)^{a.y})|y\rangle$$

$$= \frac{2}{\sqrt{2^{n+1}}}\sum_{y.a\ \text{even}}(-1)^{x0.y}|y\rangle$$

When measuring result of this state for random ‘y’ such that $y.a = o \bmod 2$. So unknown bit a_i of a must satisfy $y_0.a_0 \oplus \ldots\ldots\ldots\ y_{n-1}a_{n-1} = 0$.

We repeate this step until n linearly independent equeation have been found. we have 50 % chances of getting linearly independent equation every time this step performed. So if we repeat process 2n times then we have 50% chance that ‘n’ linearly independent equations have found.

4. Problem – Let $N = 2^n$, Alice and Bob are each given an N-bit number ‘u’ & ‘v’ respectively. The objective is for alice is to compute an n-bit number ‘a’ and Bob to compute n-bit number ‘b’ such that

$$d_H(u,v) = 0 \rightarrow a = b$$

$$d_H(u,v) = {}^{N}\!/_{2} \rightarrow a \neq b$$

$$\text{else} \rightarrow \text{no condition on a \& b}$$

Where
$d_H(u,v)$is Hamming distance between u & v.

In this problem we use entangled pair of qubits so we will not need any additional communication between Alice and Bob’s n-bit numbers.

So we have n entangled pairs(a_i, b_i)in state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ for n pairs $a_0.a_1 \ldots\ldots\ldots\ a_{n-1}, b_0, b_1 \ldots\ldots\ldots\ b_{n-1}$.So 2n state $= \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}|i,i\rangle$. Here Alice can manipulate first n qubits and Bob can do same with other n qubits.

Now Walsh Transformation W on n bits.

$$|\varphi\rangle = W(\frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}(-1)^{u_i\oplus v_i}|i\rangle|i\rangle)$$

For a=x=b probability is $|\langle x,x|\varphi\rangle|^2$
If u = v then probability is 1
If $d_H(u,v) = {}^{N}\!/_{2}$ then probability is 0
So

$$|\varphi\rangle = w^{2n}\frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}(-1)^{u_i\oplus v_i}|i\rangle|i\rangle$$

$$= \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}(-1)^{u_i\oplus v_i}(w^n|i\rangle \otimes w^n|i\rangle)$$

$$= \frac{1}{N\sqrt{N}}\sum_{i=0}^{N-1}\sum_{j=0}^{N-1}\sum_{k=0}^{N-1}(-1)^{u_i\oplus v_i}(-1)^{i.j}(-1)^{j.k}|jk\rangle$$

Now

$$\langle x,x|\varphi\rangle = \frac{1}{N\sqrt{N}}\sum_{i=0}^{N-1}(-1)^{u_i\oplus v_i}(-1)^{j.x}$$

$$= \frac{1}{N\sqrt{N}}\sum_{i=0}^{N-1}(-1)^{u_i\oplus v_i}$$

So if u = v then $(-1)^{u_i\oplus v_i} = 1$and $\langle x,x|\varphi\rangle = \frac{1}{\sqrt{N}}$, and probability summed around 1 with a=b=x for some bit string.

For $d_H(u,v) = N/2$ sum $\langle x,x|\varphi\rangle = \frac{1}{N\sqrt{N}}\sum_{i=0}^{N-1}(-1)^{u_i\oplus v_i}$ so $\langle x,x|\varphi\rangle = 0$ probability will be 0.

II. CONCLUSION

Mathematics is language of nature, so we solved most basic quantum problem with mathematical derivations and traditional theorems for better understanding of implementation of quantum algorithms . I have studied many resources on quantum computing and algorithms and them compile all the knowledge with some improvisation in this research paper . By end of reading this research paper one will be able to understand basic to intermediate quantum algorithms and how to design one. Quantum computing is vast topic so I just covered a small portion of that wide sea. Please refer reference for further understanding.

REFERENCES –

[1]. Quantum computing : A Gentle guide by Eleanor Rieffel and Wolfgang Polak
[2]. An introduction to quantum computing by Phillip Kaye, Raymond Laflamme and Michele Mosca.
[3]. The Second quantum revolution by Lars jaeger.
[4]. Mathematics of quantum mechanics by Martin Laforest.